IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TENNESSEE
WESTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	**Criminal No. 17-cr-20097-JTF**
Plaintiff,	)	
	)	
vs.	)	
	)	
JASON NEEDHAM,	)	
	)	
Defendant.	)	

UNITED STATES' POSITION ON PRESENTENCE REPORT
and SENTENCING MEMORANDUM

Comes now the Acting United States Attorney for the Western District of Tennessee, by and through Timothy C. Flowers, Trial Attorney, Computer Crimes and Intellectual Property Section, Department of Justice, and Debra L. Ireland, Assistant United States Attorney, and in submitting the government's position on the presentence report and sentencing in this matter, would show this Court the following:

I. Presentence Report

The government has no objections to the facts as stated in the presentence report or to the calculation of the advisory guideline sentence range. As calculated, the defendant's advisory sentencing range is 18 to 24 months in custody, followed by a term of supervised release not to exceed three years. Restitution is due the victim of this offense.

II. Recommended Sentence

The government recommends a sentence at the low end of the advisory guideline

range—18 months—and a one-year term of supervised release to follow. Such a sentence would be sufficient, but not greater than necessary, to reflect the seriousness of the offense, promote respect for the law, provide just punishment, promote general deterrence, and avoid unwarranted disparity among similarly-situated offenders, while also taking into consideration the nature and circumstances of the offense and the personal characteristics and history of this particular defendant.

The government is also seeking $_____ restitution for the victim of the offense, as well as forfeiture of _____property used to commit or facilitate the offense.

III. Application of § 3553 Factors

In sentencing, a court must impose a sentence that is sufficient, but not greater than necessary to accomplish several objectives; specifically, to reflect the seriousness of the offense, promote respect for the law, provide just punishment, deter criminal conduct, and protect the public. 18 U.S.C. § 3553(a)(2).

A. Seriousness of the offense

The internet is now inextricably intertwined with every aspect of modern life, affecting the ways we work, socialize, and learn. And as the electronic transmission, sharing, and storage of data becomes increasingly important to our daily activities, so too do efforts to maintain the integrity of our digital information systems. Most entities do take steps to protect their digital resources, using virtual security tools like firewalls, passwords, and encryption. But no matter how diligently applied, these precautions are simply insufficient protection—much like locks and gates are not enough to ensure security in the real world. Someone who is determined to invade a private space—digital or otherwise—will always be able to find a way around any safeguard we

put in place. We very much need the laws that criminalize cyber intrusions, and enforcing those laws is of critical importance.

In the instant case, the victim company took precautions to secure their work product—using passwords, changing them on a regular basis, limiting access to certain servers and documents, updating protocols and equipment regularly. Yet for more than two years, a former insider was able to breach the system. Business plans, proposals, budgets, engineering drawings, client lists, email—the defendant copied it all. And whether he admits it or not, possession of such information does impart a competitive advantage.

Computer intrusion crimes must also be taken seriously because they are so difficult to detect. Unlike a home burglary, for example, where a victim might notice missing items or damage to the premises, virtual invaders are not obvious. Most intrusions are not discovered until long after the damage has been done.

For all these reasons, the sentence imposed in this case needs to demonstrate that violations will be taken seriously, and offenders will face serious consequences.

B. Deterrence

In the instant case, the defendant has expressed his remorse (apparently, sincere) and assures this Court he will never again try to gain access to computers, servers, and digital spaces he is not entitled to enter. Thus, need for specific deterrence is not as compelling in this particular case as it may be in others. However, the sentence to be imposed must also deter *others* from engaging in similar conduct—and that *is* important. The sentence in this case must promote respect for the law and deterrence in general, sending a message to everyone that incidents of computer intrusion will be investigated, intruders trying to gain an edge through fraudulent access

will be held accountable, and the accounting they receive will not be insignificant.

The government's recommended sentence appropriately addresses the sentencing objectives of respect for the law, as well as general and specific deterrence.

C. Preventing unwarranted disparities in sentencing

The advisory sentencing guidelines are a starting point, a tool that places defendants with similar backgrounds, criminal histories, and offense conduct in comparable guideline ranges to ensure that no matter where criminal conduct occurs, like offenders will stand before a court with the same initial recommended range of punishment. Placement of a sentence within, above, or below the range is then determined based on the specific facts of each case and characteristics of each offender.

In the instant case, the defendant, a licensed engineer with no criminal history, pled guilty to accessing a competitor's computer without authorization repeatedly over an approximately two-year period. (Record Entry (RE) 1, Information, PageID 1; RE-6, Plea Agreement, PageID 10-13; RE-6-1, Statement of Facts, PageID 14-18.) In the past decade, sentences in comparable cases have ranged from home confinement to five years in prison. Examples include:

- *United States v. Trotter*, 478 F.3d 918 (8th Cir. 2007). The defendant pled guilty to intentionally causing damage to a protected computer without authorization. A former employee of the Salvation Army, Trotter was sentenced to 18 months for deleting files from the non-profit's computer network and shutting down the computer-operated phone system.

- *United States v. Steele*, 595 Fed. App'x. 208 (4th Cir. 2014). Steele spent nine months secretly logging in to the email server of his former employer, gaining access to confidential and proprietary information related to its contract bids, accessing the server approximately 80,000 times. A jury convicted Steele of two counts of wire fraud and fourteen counts of unauthorized access to a protected comptuer. Steele was sentenced to 48 months.

- *United States v. Snowden*, 806 F.3d 1030 (10th Cir. 2015). Snowden pled guilty to

obtaining information from a protected computer without authorization and intercepting email. Snowden logged into his former employer's computer system "dozens of times" using someone else's password and copied data and about 20,000 emails. He was sentenced to 30 months.

- *United States v. Musacchio*, 590 Fed. App'x. 359 (5th Cir. 2014) (*abrogated on other grounds*) (*judgment affirmed*, -- U.S. --, 136 S. Ct. 709 (2016)). Musacchio accessed the computer servers of his former employer without authorization, gaining access to confidential and proprietary information related to its contract bids. After trial, Musacchio was sentenced to 60 months.

- *United States v. Nosal*, 844 F.3d 1024 (9th Cir. 2016). Nosal left his employer to start a competing business, but continued to access company computer files using the credentials of another person. A jury convicted Nosal of accessing a protected computer without authorization and theft of trade secrets; Nosal was sentenced to a year and a day in prison.

- *United States v. Buchanan*, 586 Fed. App'x. 145 (4th Cir. 2014). Buchanan pled guilty accessing a protected computer without authorization and received an 18-month sentence.

- *United States v. Batti*, 631 F.3d 371 (6th Cir. 2011). Batti accessed without authorization confidential files of the CEO of the advertising firm where he worked and copied the files. Batti was fired, and after his access was rescinded, he gained access to the company's server and email by guessing a password. Batti was convicted in a bench trial and sentenced to one day in prison and three years' supervised release with the first six months on home confinement.

- *Lanam v. United States*, 554 Fed. App'x. 413 (6th Cir. 2014). Lanam, an information technology professional, used the computer system of one of his clients to attack the computer system of one of his former clients. After a jury trial, Lanam was sentenced to 21 months and ordered to pay restitution.

- *United States v. Correa*, No. H-15-679 (S.D.Tx. 2016) (*available at* https://www.si.com/mlb/2016/07/18/cardinals-chris-correa-hacks-astros-prison-sentence, *last accessed* July 11, 2017.) Correa was sentenced to 46 months after accessing without authorization the scouting records and analysis of the Houston Astros for the benefit of the St. Louis Cardinals.

The sentence recommended by the United States in the instant case is in line with sentences imposed in similar cases. Neither unnecessarily harsh, nor disproportionately lenient, it would satisfy the need to provide just punishment, promote respect for the law, and perhaps most importantly, act as a deterrent. In a digital world where highly confidential, personal, and

valuable information can be collected surreptitiously, potential victims need to know that the law protects and respects their property and privacy—even in digital form—and to warn individuals like the defendant that computer hacking has real consequences.

IV. Restitution

Crime victims have the right to full and timely restitution as provided by law. 18 U.S.C. § 3771. For certain offenses, including any offense against property and any offense in which an identifiable victim has suffered physical injury or pecuniary loss, restitution is required under the Mandatory Victim Restitution Act (MVRA). 18 U.S.C. § 3663A(a)(1); (c)(1)(A)(ii) & (c)(B). For purposes of restitution a "victim" is a person directly and proximately harmed by the defendant's criminal conduct. 18 U.S.C. § 3663A(a)(2).

Under the MVRA, an order of restitution in a property crime shall require return of the property, if that is possible, or reimbursement in an amount equal to the value of the property on the date of damage, loss, or destruction or the date of sentencing, whichever is greater, less the value of any portion of the property that is returned. 18 U.S.C. § 3663A(b)(1). In all cases, victims should be reimbursed for lost income and necessary expenses for childcare, transportation and other expenses incurred due to participation in the investigation and prosecution of the offense. 18 U.S.C. § 3663A(b)(4). Generally, restitution under the MVRA covers directly related to the defendant's conduct, but not consequential damages. *See United States v. Bogart*, 490 Fed. Supp 2d 885, 894 (E.D. Oh. 2007) (noting that the majority of Circuits have found consequential damages cannot be included in restitution under MVRA) (judgment affirmed by *United States v. Bogart*, 576 F.3d 565 (6th Cir. 2009)). Consequential damages are those that do not flow "directly and immediately" from an injurious act but result indirectly from that act. *Id*.

(internal quotations omitted).

When it comes to computer crimes however, the "property" at issue is not always damaged in the traditional sense. Thus, the Computer Fraud and Abuse Act (CFAA) includes more tailored definitions of "damage" and "loss." For CFAA purposes, "damage" means "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). "Loss" includes "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11); *Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC*, 774 F.3d 1065, 1073 (6th Cir. 2014). This is so regardless of whether the loss was reasonably foreseeable. U.S.S.G. § 2B1.1 com. n. 3(A)(v)(III). However, losses must be actual—intended loss as factored into the guideline calculations is not included. *United States v. Healy* 553 Fed. App'x. 560, 567 (6th Cir. 2014); *United States v. Simpson*, 538 F.3d 459, 465-66 (6th Cir. 2008) (internal citations omitted). Therefore, "loss" for restitution purposes is not necessarily identical to the "loss" calculated under the Sentencing Guidelines for establishing an advisory sentencing range. *United States v. Nosal*, 844 F.3d 1024, 1046 (9th Cir. 2016). This makes sense, because the purpose of restitution is to make the victim whole, while the Guideline calculations establish the defendant's relative culpability as compared to other offenders. *Id*.

In CFAA cases, courts have upheld restitution to cover the cost of notifying victims that their personal information had been stolen (*United States v. Phillips*, 477 F.3d 215, 224-25 (5th Cir. 2007)); the cost of credit monitoring for individuals victimized by theft of personal

information (*United States v. Janosko*, 642 F.3d 40 (1st Cir. 2011)); and legal fees (*United States v. Steele*, 595 Fed. App'x. 208, 216 (4th Cir. 2014)). Courts have rejected, however, restitution for lost revenue *unless* the loss is due to an interruption of service caused by the defendant's actions. *Nexans Wires S.A. v. Sark-USA, Inc.*, 166 Fed. App'x. 559, 563 (2nd Cir. 2006); *see also ES & H, Inc. v. Allied Safety Consultants, Inc.*, 2009 WL 2996340, No. 3:08-cv-323 (E.D.Tenn. 2009).

In the instant case, defendant pled guilty to a CFAA violation. He has agreed to make restitution in the amount of $142,641.06, which covers the victim's reasonable cost of assessing damage and restoring its computer system ($127,416.44), legal fees related to the offense conduct ($8,866.45), replacement of software and hardware ($3,418.17), and the cost of providing identity theft protection and monitoring for one year for employees whose email accounts were compromised by the defendant's actions.[1] The victim has identified an additional $6,757.18 in compensable loss and damage for legal fees and $22,995.47 in labor costs that had not yet been incurred at the time the plea agreement was finalized. The government asks that restitution be ordered for these losses, in addition to that which defendant has already agreed to pay.

The victim company also seeks to recover lost revenue of $140,756.55 for six projects defendant's company won over the victim company during the time period defendant had access to the victim's private information. In the context of lost revenue—otherwise characterized as ill-gotten gains from illegal conduct—restitution is generally inappropriate. *See United States v. Kilpatrick*, 798 F.3d 365 (6th Cir. 2015) (explaining that the defendant's gains from a RICO and extortion scheme were inappropriate for restitution). This is because courts prefer that parties

1 The agreement covers one year of monitoring for the affected employees. (Record Entry (RE) 6, Plea Agreement, PageID 10-13, para. 12.) The victim company purchased three years of credit monitoring for affected employees at a cost of $2,940.00. (RE-12, Presentence Report - Final, PageID 43-62, para. 22.)

litigate a defendant's ill-gotten gains through civil litigation. *See United States v. Fair*, 699 F.3d 508, 514 (D.C. Cir. 2012) (explaining that victims may generally "achieve disgorgement of . . . ill-gotten gains through other statutory and civil-recovery mechanisms"); *see also United States v. Stanley*, 309 F.3d 611, 613 (9th Cir. 2002) (holding MVRA does not allow "double recovery by a victim").

Finally, the victim seeks restitution based on the value of the 82 dwg files the defendant copied from the company's computer system. Estimating the cost to produce each at between $2,000 and $3,000 dollars, they request between $164,000 and $246,000. The cost of developing proprietary information may be considered when estimating amounts of loss or intended loss for guideline calculation purposes. U.S.S.G. § 2B1.1(C)(ii). So can reduction in the value of the information, so long as it is a result of the offense. *Id*. Restitution, however, requires return of the property or, if return is impossible, impractical, or inadequate, monetary compensation for the greater of the value of the property on the date of the damage, loss, or destruction or the value of the property on the date of sentencing less the value of any part of the property that is returned. 18 U.S.C. § 3663A(b).

In the case at bar, the victim company continues to possess and make use of its intellectual property, the dwg. files. And although the company has endured "loss" in that its control over who, if anyone, gets to see its plans, documents, budgets, and ideas, erosion of this right of determination is not necessarily pecuniary harm that can be remedied through restitution. This loss can be mitigated, however, through forfeiture and destruction of the materials defendant took from the

Consequently, the government maintains that the agreed-upon $142,641.06 restitution

amount, amended to include an additional $29,752.47 for compensable losses not included in the initial accounting of damages, is the more appropriate amount of restitution due.

III. Forfeiture

In imposing sentence for an offense under the CFAA, a court shall order that the defendant forfeit his interest in personal property that was used or intended to be used to commit or facilitate commission of the offense, and any property, real or personal, constituting or derived from, any proceeds the defendant obtained directly or indirectly as a result of the violation. 18 U.S.C. § 1030(i) & (j). The government seeks forfeiture of items removed from the defendant's home and place of business that contain information, drawings, email, or documents obtained from the victim company, as well as destruction of any hard copies of said documents. The items are specifically identified in the attached search warrant returns and incorporated herein by reference.

WHEREFORE, PREMISES CONSIDERED, the United States moves the Court to sentence in accord with the government's recommendations.

Respectfully submitted,

LAWRENCE J. LAURENZI
Acting United States Attorney

By: /s/ Debra L. Ireland
Assistant United States Attorney

CERTIFICATE OF SERVICE

I, Debra L. Ireland, Assistant United States Attorney, do hereby certify that a copy of the foregoing Motion was forwarded by electronic means, via the Court's Electronic Filing System, to Charles Mitchell, Attorneys for Defendant.

This 18th Day of July, 2017.

/s/ Debra L. Ireland
Assistant United States Attorney